Page 3960 - 3972

***DOI:** https://doij.org/10.10000/IJLMH.1110282*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 3

2025

A Study of Cyber Crimes and its Impact

MAYURI SINGH[1]

ABSTRACT

Every nation's economic growth is significantly influenced by the role that banks play. The economy would not function without its banks. The bank is not only an institution but also one of the fundamental requirements of humans in the modern day. Everyone has a need for banks, and our identity is established via our bank accounts. The financial sector in India is undergoing rapid expansion and change at an alarming rate, with new laws, rules, and regulations being implemented almost on a daily basis. The reserve bank of India exercises oversight over the Indian banking system and has system holdings. In the modern day, bank accounts are considered to be human common things; hence, they may be utilised whenever and whenever. The banker has observed and analysed the desires and satisfaction of the client, such as rapid changes in the method transaction channels such as ATM, balance inquiry, online banking, mobile banking e cheque, electronic money transfer, credit cards, debit cards, smart cards, and payment banks. The Indian bank began operations in the post office sector in addition to establishing a number of payment banks. Since the Post Office Department is now employing banking services, this indicates that the Indian Banking Sector is undergoing significant transformation and expansion.

Keywords: *Laws, Rules, Nation, Banking, Finance, Growth*

I. INTRODUCTION

The growth of India's banking industry can be traced back to reforms made in the final decade of the last century that made the market more accessible to private and foreign investment. Financial dealings have gone digital over the past two decades. The introduction of ATMs, online/mobile banking, and more recently payment gateways/aggregators have revolutionised the way we conduct financial transactions. Instead, globalisation and technological progress have changed the face of fraud in India and around the world. Concerns about regulation and prevention have been raised as new forms of fraud have emerged to replace older ones.[2]

Because of the increased reliance on technology in modern banking, both internal and external fraud have increased. Mobile banking, payment banks/aggregators like PayTM, and payment gateways like Citrus Pay, and CC Avenue have all seen rapid growth in India, making banking activities and other payment options more accessible but also increasing the risk of

[1] Author is an Assistant Professor at Classic College of Law, India.

[2] Bessis, Joel, "Risk Management in Banking." Third Edition, John Wiley & Sons Ltd. (2010).

fraud. Banking has always played a crucial role in any nation's economic development because of its central role in trade and commerce. Moneylenders and merchants, who provided financial services before the advent of the organised banking sector, were often unchecked and prone to fraud and corruption. The establishment of the Bank of Bombay in 1720 and the Bank of Hindustan in 1770 marked the start of the modern era of banking in India. Since then, banking has drastically changed, moving from being passive stewards to active promoters of economic growth. Nowadays, businesses and investors can easily transfer money thanks to the modern banking system. Financial institutions such as banks and credit unions provide a wide range of services to the government, as well as to individuals, small businesses, and multinational corporations. Banking and financial institutions are the economic engines that power any country's financial sector.

With an increase in both opportunities and potential fraud risk areas, this new role carries heavier burdens of responsibility and accountability for the financial sector as a whole. Large-scale bank investments in corporations and businesses come with an increased risk of internal and external fraud on top of the usual business risks. A brief overview of banking in India is provided by the RBI, which was established in 1934 with the goals of regulating the monetary system, ensuring monetary stability, and managing the nation's credit system.

After the RBI was nationalised in 1949, other banks in operation at the time were also nationalised in 1969 and 1980, ushering in a period of profound change that saw banks pivot from serving purely commercial interests to aiding the welfare state and promoting economic growth. Another shift in the banking sector's paradigm occurred as liberalisation policies were put into effect in the final decade of the twentieth century. Banks had to keep up with the various banking standards adopted and utilised by global competitors, in addition to the rapidly changing technological landscape.

To "receive deposits of money from the general public for lending or investing the same and which is repayable on demand or otherwise to the depositors" is outlined in Section 5(b) of the Banking Regulation Act of 1949 as the interpretation of banking. Financial institutions are granted permission to conduct additional business activities in Section 6 of the Act.

It is crystal clear from the provisions of the aforementioned Act that banking today entails far more than just deposits and loans. The banking industry's enhanced efficiency has led to a general improvement in business practices. Indian financial institutions were also compelled by globalisation and liberalisation to become more familiar with global banking standards.

India entered a new technological and economic era in the last decade of the twentieth century. Nowadays, technology is not only fundamental to our daily lives but also the bedrock of all commercial endeavours. The banking sector has heavily invested in technology, expanding the range of available channels for customers to make their financial dealings with complete ease. FinTech, which refers to any technological advancement in the financial services industry that makes use of Information Technology (IT), is now a major factor in the way banking operations are carried out in areas like asset management, borrowing and lending, payments and settlements, insurance, and so on. Payment aggregators and gateways are two examples of cutting-edge technology that have sped up the settlement and processing of retail and wholesale payments.[3]

Respectfully maintaining pace with the rest of the world, India has advanced and adapted to technological advances in banking operations. The rapid but commendable shift from traditional, manual banking, in which the bank required customers to make personal appearances premises for any transactions, to modern digital banking in India, has been complicated by the layering of systems, the introduction of new risks, and the proliferation of E-Banking frauds. The increased reliance on automated systems increases the risks of internal and external cybercrime or fraud and results in the need for frequent upgrades to keep up with rapidly evolving technology and the complexity of integrating different platforms.

II. Problem on hand

Despite all of the benefits of e-banking, technological advancement has presented the banking industry with a number of challenges. Operational risks, technological issues, security issues, and legal issues are the primary causes of the numerous problems encountered when using e-banking services. Unauthorized data access, data theft by hackers, and data loss or damage caused by viruses are just a few of the many security issues that people face. The online banking system is undergoing maintenance issues. Inexperienced personnel are required to manage the electronic banking system. In addition to enhancing the likelihood of committing e-banking fraud, problems with literacy and a lack of computer literacy also increase the likelihood of committing such crimes. If salami attacks are possible, funds may be fraudulently transferred from one person's account to the fraudster's account using specialised software. E-banking has provided customers with convenient banking services and made their lives easier, but it has also introduced new risks that could affect the banks' profitability, capital, and reputation, as well as cause customers to incur financial losses. These risks may also present bank executives with a number of risk-related challenges. The lack of qualified

[3] Shah, Mahmood, "E-Banking Management: Issues, Solutions and Strategies," New York, Information Science Reference. (2009).

personnel to manage the system for providing e-banking services is one of the challenges facing the e-banking industry.

Due to the universal accessibility of internet banking, there are no geographical restrictions. Internet banking services have an unlimited geographical reach. As a result, it is difficult to identify and control criminals who commit fraud via online banking.

In order to reduce the incidence of e-banking fraud in India, preventative measures are necessary. Moreover, laws, rules, and regulations must be written correctly. There are regulatory and supervisory challenges associated with the banking industry's adoption of new technology. Cross-border banking transactions exacerbate these difficulties because they raise jurisdictional and legal issues that must be addressed when addressing or resolving e-banking fraud cases. Although there are legal provisions in place to combat ebanking fraud, modifications will be necessary because it is possible that as more people use e-banking services and e-banking activity expands, new legal issues will emerge.

If you violate or fail to comply with established rules and regulations, you expose yourself to legal risk. Inaccurate application of the law can occasionally result in legal complications. The cyber laws of India are inadequate to combat e-banking-related crimes. There is a chance that the laws and regulations of multiple nations or states will overlap due to the internet's expanded geographic reach. Different states and nations are subject to different laws. Consequently, the question is which laws ought to be applied to cross-border issues or frauds. In an internet banking service system, banks have limited discretion to stop payments based on customer instructions. The United Kingdom has more codified laws governing e-banking services than India. The Electronic Funds Transfer Act is a United Kingdom statute governing electronic money transfers. Developed nations, as opposed to developing nations such as India, also have more advanced data protection laws pertaining to maintaining the privacy of customer personal information. Internet banking has numerous benefits, but it also has some drawbacks. Using various techniques such as hacking, cracking, etc., a large number of fraudsters have discovered and successfully exploited online banking accounts. Fraudsters gain access to the user's computer system by compromising the Internet service provider's address, Domain Name Server, etc. They then gain access to and steal sensitive data and information, which they use to generate substantial profits from the victim's bank account. Hacking is possible from any location on Earth without fear of being discovered. This issue can be resolved only through the use of superior technology, regular technological advancements, and efficient and effective legislative measures.[4]

The problem persists because the existing legal provisions are ineffective against the fraudsters who commit these types of frauds, despite the fact that many steps have been taken to stop these types of activities through legal provisions.

A hacker is a person who engages in hacking. A hacker, also referred to as a computer expert, gains access to a user's computer by breaking into it and stealing information that can be used to commit fraud and cause financial losses. Utilizing online banking is fraught with peril. If the password or other user information is compromised, hackers can gain access to the user's account and use the information they obtain to commit fraud against the user, costing them a significant amount of money. By the time customers receive their bank account statements and discover unauthorised transactions, it will be too late and difficult to locate the fraudster.

III. CONCEPT AND CLASSIFICATION OF CYBER CRIME

New types of criminal activity are on the rise due to the widespread availability of the Internet. Some of them include "computer hacking, software piracy, online paedophilia, industrial espionage, password cracking, spoofing, telecommunication fraud, e-mail bombing, spamming, pornography, and the accessibility of illegal or unauthorised items and services." A number of brand-new problems have emerged in recent years, including online credit card fraud, cyber terrorism, money laundering, and unauthorised use of encrypted Internet connections. There is a significant danger of unauthorised bank withdrawals and money laundering activities due to the present inadequate electronic payment system, which lacks sufficient restrictions.

The modes of committing the crime are evolving dramatically as the human mind evolves daily. Criminals are leveraging their growing intelligence to devise ever more sophisticated methods of committing crimes and evading arrest. No one foresaw computers being a breeding ground for or facilitator of crime. "Father of the Computer" Charles Babbage surely had no idea that his creation would one day be used for criminal purposes or to do damage to society. The term "cybercrime" is often used to refer to any wrongdoing committed through a compromised computer system. Incorrect definitions of "cybercrime" have been widely used. No Act or Statute made by the Indian Parliament provides a definition for this term. Cybercrime is conceptually related to "real world" crime. Both include some kind of action or inaction that leads to a breach of the law and, in response, the state imposes some kind of punishment. Despite the fact that cybercrime is a relatively new sort of crime that began not

[4] Singh, S. (2007). "Banking Sector Reforms in India." New Delhi, Kanishka Publishers.

long after the introduction of computers, the issue has worsened as a result of the internet's pervasive presence in modern life.

CONVENTIONAL CRIME

Crime has always been a part of human society and the global economy. A criminal offence is anything defined by the law. In legal parlance, a crime (sometimes spelt “offence”) is “a legal error that may be followed by criminal conduct that may result in punishment.” Lord Atkin once said that breaking the law was a defining feature of criminal behaviour. Only by considering the kinds of behaviour that carry legal penalties can we determine whether or not an act has criminal potential. To commit a crime, one must first engage in conduct that is prohibited by law and whose infraction carries criminal penalties.[5]

CYBER CRIME

Cybercrime is the newest and most complicated issue facing the online community at large. The term “cybercrime” refers to any criminal act that takes place online and involves the use of a computer in some way, with the “traditional” form of crime serving as the “genus” for these online offences. The term “cybercrime” refers to any unlawful activity that makes use of a computer, whether for the purpose of committing an instrumentality target or as a means of maintaining more criminal activity. One potentially all-encompassing definition of cybercrime is “unlawful action in which the computer is either a tool or a target, or both.” Computers may be used to perpetrate a wide variety of unlawful activities, including monetary theft, the selling of illicit items, pornography, online gambling, theft of intellectual property, spoofing of electronic mail, forgery, cyber defamation, and cyber stalking.

IV. Reasons for cyber crimes

The following are some of the reasons why computers are vulnerable to cybercrime:

HUGE DATA STORAGE CAPACITY The computer has the unique ability to store massive amounts of data in a very small amount of space. In a CD-ROM, a little microprocessor computer chip can hold lakhs of pages. This storage capacity provides ample area to easily remove or derive information via physical or visual means. Even if the power is switched off, any data stored in ROM will stay intact.

WIDE ACCESS TO INFORMATION Because it relies on complicated technology rather than simple human acts, a computer is an electronic device. It is the widest range of information resources available via big and extensive media which is the greatest benefit of

[5] International Journal of Cyber Criminology (ISSN: 0974-2891).

networking in the computer age. Networks are increasingly being used by businesses to make information readily available to their employees, customers, and other parties with whom they interact. This is why networking and cyber activities are becoming more and more commonplace in today's information-driven society.

THE COMPLEXITY OF COMPUTER SYSTEM The operating systems of the computers are made up of millions of codes, and the operating systems themselves are made up of millions of codes. At every point in the process, the human mind is susceptible to error. This vulnerability is exploited by cyber thieves, who infiltrate the computer system. Hackers are criminals who take advantage of the flaws in current operating systems and security measures.

NEGLIGENCE OF NETWORK USERS Human behaviour is intimately linked to the prevalence of neglect in the world. Consequently, it is quite likely that the owner or user of the computer system may make an error or neglect in securing the system, allowing a cybercriminal to acquire access or control of the system without authorization or consent.

NON AVAILABILITY & LOSS EVIDENCE It has been supplanted by digital computer processing and network technologies for the production, storage, transmission, and distribution of information or records. The most pressing issue for law enforcement and investigators is how to acquire and retain evidence. Cybercrimes are different from other types of criminal offences in that gathering enough evidence to prove an accused person's guilt beyond all reasonable doubt is much more difficult. It is difficult to establish a criminal case against a cybercrime due to the anonymity that is provided by the internet.

V. NEED OF CYBER LAW

Intellectual property violations, piracy, freedom of expression, jurisdictional issues, etc. are just some of the many legal issues that have arisen as a result of the growing importance of e-commerce and e-governance on the internet and other forms of computer or digital processing devices, and they all require the multifaceted approach of the interdisciplinary legal community to resolve. Cyberspace transactions of citizens inside a country's territorial jurisdiction provide a major problem to law enforcement organisations because it lacks any physical features such as sex, age, or gender. There are times when the conventional assumption that an internet user is governed by local law does not apply because of the nature of the issue, which is transnational in scope. Even in the early days of the internet, no one imagined that it could be unintentionally utilized for criminal objectives by internet users.

VI. Major issues in internet banking

The rule of law simply cannot be expected to keep up with the rapid development of new technologies. The current scandal involving online snooping exposed, among other things, the weakness and insufficiency of legislation regulating internet usage. There is no suggestion that the difficulties of determining jurisdiction, fixing culpability, and recording and reproducing evidence will soon be resolved. As more institutions in India go towards electronic banking, worries about security and abuse have grown.

Although banks were encouraged to start out serving the public good, they have always been run as businesses with profit maximisation as their primary goal. Issues have surfaced in the banking sector in recent years as a result of the broad implementation of new economic settings such as globalisation, liberalisation, and privatisation. Deregulation, advances in technology, and globalisation are all factors that are having a significant impact on the financial services available in India.

As a direct result of the proliferation of online banking, a number of conventional financial institutions have revised their IT strategies. It has been stated that the costs associated with offering online banking services are lower than the costs associated with maintaining branch banking, and that financial institutions who do not adapt to the changing market are likely to see a loss in customer base

VII. Technological challenges to banking sector in India

The Indian banking sector has undergone significant transformation as a result of the liberalisation and deregulation process that began in 1991–1992. We've made the transition from a highly controlled setting to a more market-based, competitive one. The term “information technology” (or “IT”) has become ubiquitous in recent years. The rapid development of technology has shrunk the globe into a global village, and it has also brought about significant shifts in the financial sector. In today's increasingly globalised, liberalised, privatised, and competitive market, banks must function. Because of Technology, a new paradigm in business has emerged. It is becoming more important in enhancing banking sector offerings.

VIII. Initiatives taken so far to handle cyber crime prevention in India

There is now a strategy in place for cyber security measures as part of the 12th Five-Year Plan (2012–17). This plan focuses on the following key areas:

- Collaboration

- Framework laws that allow for
- Detection, prevention, and mitigation of security incidents via raised awareness, better training, and more rapid reaction times
- The Compliance, Assurance, and Policy of Security
- Scientific investigation towards the improvement of security

NATIONAL CYBER SECURITY POLICY, 2013

To combat cybercrime, the Indian government adopted this policy in 2013. The goal of this text is to ensure a safe and secure internet for Indian residents. It is the goal of the Cyber Security Policy to safeguard data in cyberspace by reducing vulnerabilities and reducing the likelihood of cyber events, as well as the harm caused by them. If implemented, it will ensure that consumers have the confidence to use electronic payment systems because of secure computing infrastructure. Cyber security intelligence will become a vital part of anticipating attacks and swiftly implementing countermeasures when applied at the macro level.

ONLINE COMPLAINTS

The Central Government has recently proclaimed that an “Inside Citizen Portal” will be established in response to Supreme Court inquiries on measures taken to combat cybercrime. Residents will be able to document their experiences with various forms of cybercrime, such as digital stalking and money-related extortion, online. For example, any complaint that is made on a portal will be flagged by the police, who can then track and update its status. The governmental response describes this process. The complainant will be given the option to view updates and bring his complaint to the attention of superiors.

CYBER POLICE STATIONS

State and district cybercrime coordination cells, cyber forensics, and mobile forensics labs have been mandated by the Union Home Ministry as part of an eight-point set of instructions to combat cybercrime. District cybercrime cells will report to the district SP, but the State Cyber Crime Controller will provide direction to the state cybercrime coordination cells. Several states' Criminal Investigative Departments have cybercrime investigation units (CID). To effectively combat cybercrime, state governments have been urged to provide the necessary technology infrastructure as well as human resources to ensure that cybercrime can be detected early, registered, investigated, and punished. In addition, a national centre of excellence for cyber forensic services and training has been established, as well as a national research and training centre.

CRIME CRIMINAL INFORMATION SYSTEM [CCIS]

To store and retrieve criminal records, the Indian government created the Crime Criminal Information System. 2005 saw the implementation of CCIS MLS, a version of the system that allows for the simultaneous use of five regional languages on the web. Data warehousing for criminal analysis has also been introduced. So that investigators and supervisors can access CCIS MLS databases at the national and state levels from anywhere, at any time, the web-enabled application has been developed.

CYBER CRIME CELL OF CBI

"CBI has a Cyber Crime Cell which conducts inquiry of inter-state and important cybercrime cases. It has constituted a Cyber and High-Tech Crime Investigation and Training Centre at CBI Academy. To combat computer-related crimes, the CBI has the following specialized structure:

- Cyber Crimes Research and Development Unit (CCRDU);
- Cyber Crime Investigation Cell (CCIC);
- Cyber Forensics Laboratory; and
- Network Monitoring Centre.

CYBER SECURITY FRAMEWORK

A cyber security framework is a collection of papers outlining norms, rules, and recommended methods for handling cyber security threats. The purpose of the frameworks is to protect a company from potential security flaws that might be exploited by malicious parties like hackers. The word "framework" in the name gives the wrong impression and refers to software rather than hardware. Not helping things is the use of the word "mainframe," which may suggest a physical network of computers and storage devices.

According to their intended purpose, frameworks may be placed into one of three categories:

- Creates a framework for the company's cyber security initiatives
- Includes a standard set of safety measures
- provides an analysis of the current condition of the system and its technologies
- place importance on putting in place security measures

Program Frameworks

- analyses the condition of the security programme of the company
- builds a full-fledged cyber security infrastructure
- Checks how safe the software is and how it stacks up against the competition.
- Streamlines and streamlines the cyber security team's interactions with upper management and executives.

Top Cyber Security Frameworks

There are many options to choose from when it comes to a cyber-security architecture. Here are some of the best frameworks currently being used in the market. Your option depends on the security requirements of your firm. Cyber security frameworks serve as a guide for businesses. Security teams can effectively manage their companies' cyber threats if they have the right structure in place. It is possible for a company to either modify an existing framework or create a new one on its own.

THE NIST CYBER SECURITY FRAMEWORK

The "National Institute of Standards and Technology (NIST)" produced the NIST Framework for Enhancing Critical Infrastructure Cyber security (often referred to as the "NIST cyber security framework") in response to Executive Order 13636 issued by President Obama. In order to safeguard vital American infrastructure against cyber criminals, the National Institute of Standards and Technology (NIST) was established.

When it comes to cyber defence, private companies may benefit from NIST's voluntary security standards. As part of the framework, it provides recommendations on how to both prevent and recover from cyberattacks. NIST is responsible for five distinct tasks or standards:

- Detect
- Identify
- Protect
- Recover
- Respond

THE CENTRE FOR INTERNET SECURITY CRITICAL SECURITY CONTROL

If you're looking to keep overhead low while expanding your firm over time, CIS is the way to go. This framework was developed in the late 00s to protect enterprises against cyber-crimes. Twenty controls are constantly updated by security experts from a variety of sectors (academia, government, industrial). Foundational is followed by organizational before we wrap up the framework with a look at the fundamentals. With the use of benchmarks such as HIPAA or NIST, the CIS provides enterprises that aren't obligated by mandated security regulations with a framework for enhancing their cyber security.

IX. Conclusion and suggestions

With the increase in the users of internet, the increase in cyber-crimes can also be seen. There are various kinds of cyber-crimes which are happening in day-to-day life. But the people are not aware of all such types. Majority of the people know only about hacking and virus/worms. They are not aware of phishing, defamation, identity theft, cyber stalking etc. It is the need of today's world to have knowledge about these crimes which are associated with the internet. The study shows that 48% of the respondents share their personal details with other persons even they don't know them closely.55% of respondents have agreed that their PCs are often damaged by viruses. The internet users struggled with spam emails, phishing calls and emails asking for their sensitive information like mobile no., bank account, address, etc. It is the duty of each one of us to be aware of the basic cyber security. Cyber security refers to the technologies and processes that are designed to protect computers, networks and data from unauthorized access and attacks delivered via the internet by cyber criminals.

As we are living in the digital age where every nation is looking forward to increase in the technology, it is important to be aware about the pros and cons of the ongoing evolution of the digital technology. Cybercrime are the fastest going crimes in the world where malpractices like hacking, malware, phishing, internet thefts, Trojan horses, stealing money while money transferring, etc. It is better to be safe when it come to our personal information. No matter what any personal information shouldn't be disclosed to a stranger, outsider or anyone who is not concerned to us. In India, Information Technology Act, 2000 severs as backbone for combating and promoting cyber security. Therefore each and every individual should be aware about the incident happening towards the technology and be away from the crime happening all over world. The government should spread more awareness and take more precaution as it takes care of other criminal acts.

Furthermore, the study has revealed disparities in the level of awareness and preparedness among different segments of society. While some individuals may possess a high level of awareness and actively employ preventive measures, others may lack the necessary knowledge and resources to protect themselves effectively. Therefore, efforts to enhance cybercrime awareness and promote cyber security education are essential in empowering individuals and organizations to defend against cyber threats proactively.

*****